(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2004年4月29日(29.04.2004)

PCT

(10) 国际公布号:
WO 2004/036828 A1

(51) 国际分类号[7]: H04L 12/24, 12/56

(21) 国际申请号: PCT/CN2003/000801

(22) 国际申请日: 2003年9月22日(22.09.2003)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
02144191.X 2002年10月18日(18.10.2002) CN

(71) 申请人(对除美国以外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD) [CN/CN]; 中国广东省深圳市科技园科发路华为用户服务中心大厦知识产权部, Guangdong 518057 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 张涛(ZHANG, Tao) [CN/CN]; 张忠(ZHANG, Zhong) [CN/CN]; 中国广东省深圳市科技园科发路华为用户服务中心大厦知识产权部, Guangdong 518057 (CN)。

(74) 代理人: 北京集佳专利商标事务所(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建外大街22号赛特广场七层30703王学强, Beijing 100004 (CN)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A NETWORK SECURITY AUTHENTICATION METHOD

(54) 发明名称: 一种网络安全认证方法

(57) Abstract: The invention discloses a network security authentication method. The invention first sets an authentication key for a media gateway (MG) by a media gateway controller (MGC), and set a network protocol security package. Thus MGC sends security authentication request data to MG through the security package when the security authentication is processed. MG encrypts the request data using authentication key and feeds back the calculated result to MGC. MGC determines if the authenticated GC is legally based on the authentication result. Employing the above scheme can prevent illegal or forged devices from accessing to a network. In addition, since the authentication to MG is performed by the control of MGC, which has randomness of authentication, it has higher security authentication efficiency.

(57) 摘要

本发明公开了一种网络安全认证方法，该发明首先由媒体网关控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包；这样在进行安全认证时，MGC 利用安全数据包向 MG 下发安全认证请求数据，MG 利用鉴权密钥对请求数据进行加密计算，并将计算结果反馈给MGC,MGC根据认证结果确定被认证的MG是否合法；采用上述方案能够防止非法和伪造设备的网络接入；另外，由于对 MG 的认证在 MGC 的控制下进行，具有认证的随机性，因此具有较高的安全认证效率。

WO 2004/036828 A1

一种网络安全认证方法

技术领域

本发明涉及一种网络的安全认证方法。

背景技术

在下一代网络（NGN）中，存在很多基于媒体网关控制协议（MGCP）和 H248 协议（另一种媒体网关控制协议）的媒体网关（MG），这些设备分布在企业或用户家中，具有面广、量大、基于动态 IP 的特点。但在目前的 NGN 网络中，由于 MGCP 协议的应用层无安全认证机制，所以使用 MGCP 协议的 MG 安全性较差；在 H248 协议中，尽管在应用层中有安全认证机制，即在每个 H248 协议事务请求消息中可以加入安全头，在其事务响应消息中返回安全认证结果，但是该安全认证机制要在 MGC 和 MG 中要交互大量 H248 消息，大约要增加 40%的 H248 消息编解码处理时间，这使得现有的 H248 协议提供的安全认证方案大大降低了网络系统的效率，实际应用的可行性较差。因此，目前 NGN 网络存在的仿冒 MG，对 MGC 进行攻击等系统安全问题还没有得到妥善的解决。

发明内容

本发明的目的在于提供一种能够对 NGN 网络进行有效的安全认证的方法。

为达到上述目的，本发明提供的网络安全认证方法，包括:

步骤 1：媒体网关控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包；

步骤 2：在进行安全认证时，MGC 利用数据包(Package)向 MG 下发安全认证请求数据，MG 利用鉴权密钥对请求数据进行加密计算，并将计算结果反馈给 MGC；

步骤 3：MGC 根据认证结果确定被认证的 MG 是否合法。

所述网络协议为媒体网关控制协议（MGCP）或 H248 协议。

所述数据包包括：安全认证请求信号和安全认证结果事件；所述安全认证请求信号中包括安全认证参数；安全认证结果事件中包括安全结果认证参数。

所述步骤 2 进一步包括：

步骤 21：MGC 下发数据包中的安全性认证请求信号给 MG；

步骤 22：MG 收到安全认证信号中的安全认证参数，使用鉴权密钥对上述参数进行加密计算，然后将加密计算结果通过数据包中的安全认证完成事件的安全结果认证参数上报给 MGC。

由于本发明采用媒体网络控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包用于 MG 的安全认证，因此能够防止非法和伪造设备的网络接入；另外，由于对 MG 的认证在 MGC 的控制下进行，或者说在 MGC 认为需要安全认证的时候进行安全认证，这样的认证方式具有随机性，具有较高的安全认证效率。

具体实施方式

下面对本发明作进一步详细的描述。

本发明所述的方法是实现 MG 的安全管理，其实质是，为每一个 MG 配置一个鉴权密钥，当 MGC 发起鉴权请求时，MGC 将向 MG 发一个随机数，MG 根据 MGC 发来的随机数和 MG 配置的鉴权密钥（当然还可以包括其他信息），实施加密计算，返回加密结果给 MGC。MGC 实施相同的计算，判断是否与 MG 发送的加密结果相同。如果不相同则认为 MG 为非法。

本发明可以基于 H248 协议或 MGCP 协议实现，为此需要增加 MGCP 协议或 H248 协议安全数据包，所述安全性数据包是安全性认证信号和事件的集合，本发明采用的 H248 协议或 MGCP 协议的安全性认证包中包括一个安全性认证请求信号和安全性认证完成事件。安全认证请求信号中包括一个安全性认证参数；安全性完成事件中包括一个安全性认证结果参数。当 MGC 要对 MG 进行安全性认证时，MGC 下发安全性认证请求信号给 MG，同时检测 MG 的安全性认证完成事件。当 MG 收到 MGC 下发的安全性认证信号，根据配置在 MG 上的鉴权密钥和收到的 MGC 安全性认证请求信号中的参数进行加密计算。当完成加密计算，MG 向 MGC 上报安全性认证完成事件，在安全性认证完成事件的参数中上报安全加密计算结果。MGC 收到 MG 上报的安全性认证完成事件后，比较 MG 上报的安全性认证完成事件参数中的加密计算结果是否与 MGC 本身计算的加密结果相同。如果不相同则认为是非法的 MG。

下面举例说明上述过程。

采用 MGCP 协议实现本发明的 MGCP 协议安全数据包具体内容为:

数据包名称: Auth; 数据包版本: 1;

包中包含的事件:

1: 安全认证结果事件

事件名称: authoc;

检测事件参数编码: 32*64(十六进制数);

说明: 检测事件参数用于返回认证结果;

包中包含的信号:

1: 安全认证请求信号

信号名编码: authreq;

信号参数编码: 32*64(十六进制数 32 到 64 位);

上述安全认证请求信号参数即为 MGC 向 MG 发出的一个随机数。本例中,随机数为大于 16 位的字符串小于 32 位的字符串。每一位字符串 ABNF(扩展的巴科斯范式)编码为 2 个十六进制数。

基于上述数据包的认证过程及采用的伪代码为:

步骤 11: MGC 向 MG 发起认证请求: MGC 下发请求通知命令(RQNT)给 MG, 分配事务标识(100)和请求标识(123), 要求 MG 检测安全认证完成事件(auth/authoc), 同时下发安全认证请求信号(auth/authreq), MGC 生成一个 16 字节的随机数(0x78 0x90 0xab 0xcd 0xef 0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32)

作为安全认证请求信号的安全认证参数。

步骤 12：MG 收到 MGC 下发的请求通知命令（RQNT）后回送此命令的正确响应，响应码为正确响应（200），事务标识（100）与 MGC 下发的请求通知（RQNT）命令的事务标识一致。证明 MG 已正确收到 MGC 下发的请求通知命令（RQNT）。

步骤 13：MG 收到 MGC 下发的请求通知命令（RQNT）后发现有安全认证请求信号，开始进行安全认证计算，MG 取出安全认证请求信号中的参数和配置在 MG 上的鉴权密钥（该鉴权密钥假设为：0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32）进行加密计算。经加密计算，加密计算结果为（0x12 0x 34 0xab 0xcd 0xef 0xab 0xef 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88），MG 产生安全认证完成事件，MG 查看是否 MGC 要求上报加密完成事件，MG 发现 MGC 要求上报该事件，MG 上报通知命令（NTFY）给 MGC，检测到事件为安全认证完成事件（auth/authoc），事件参数为加密结果。请求标识（123）与 MGC 下发的请求通知命令（RQNT）的请求标识一致，同时分配事务标识（200）。

步骤 14：MGC 收到 MG 上报的通知事件后，回送通知命令的正确响应，响应码为正确响应（200），事务标识（200）与 MG 上报的通知命令（NTFY）的事务标识一致。证明 MGC 已正确收到 MG 上报的通知命令（NTFY）。

步骤 15：当 MGC 收到 MG 上报的加密结果，与自己计算的加密结

果比较，如果 MG 上报的加密结果与 MGC 自己计算的加密结果一致。则认为该 MG 为合法的 MG，如果不一致或者 MG 在规定的时间内没有上报自己的加密结果，则认为该 MG 为非法的 MG。

采用 H248 协议实现本发明的 H248 协议安全数据包为：

数据包名称：auth；数据包版本：1；

数据包中的事件：

1：安全认证结果事件

事件名称：authoc（0x0001）；

检测事件参数名：认证结果；

参数名称：Res ；

参数值 ABNF 编码：32*64(32 到 64 位的 16 进制数)；

参数值 ASN.1(抽象符号表示法)编码：OCTET STRING(SIZE(16..32))；(16 到 32 位的 8 位位组)；

数据包中包含的信号：

1：安全认证请求信号

信号名标识：authreq

信号参数名：请求参数

参数名称：parm

参数值 ABNF 编码：32*64(HEXDIG)

参数值 ASN.1 编码：OCTET STRING(SIZE(16..32))

基于上述数据包的认证过程及采用的伪代码为

步骤21:MGC向MG发起认证请求:MGC下发请求修改命令(modify)给MG，分配事务标识（100）和请求标识（2223），要求MG检测安全认证完成事件（auth/authoc），同时下发安全认证请求信号（auth/authreq），MGC生成一个16字节的随机数（0x78 0x90 0xab 0xcd 0xef 0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32）作为安全认证请求信号的安全认证参数。

步骤22：MG收到MGC下发的修改命令（modify）后回送此命令的正确响应，事务标识（10001）与MGC 下发的修改命令（modify）的事务标识一致。证明MG已正确收到MGC 下发的修改命令(modify)。

步骤23：MG收到MGC 下发的修改命令（modify）后发现有安全认证请求信号，开始进行安全认证计算，MG 取出安全认证请求信号中的参数和配置在MG上的鉴权密钥（假设该鉴权密钥为：0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32）进行加密计算。经加密计算，加密计算结果为（0x12 0x 34 0xab 0xcd 0xef 0xab 0xef 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88），MG产生安全认证完成事件，MG查看是否MGC要求上报加密完成事件，MG发现MGC要求上报该事件，MG上报通知命令（NTFY）给MGC，检测到事件为安全认证完成事件（auth/authoc），事件参数为加密结果。请求标识（2223）与MGC下发的修改命令（modify）的请求标识一致，同时分配事务标识（10002）。

步骤24：MGC收到MG上报的通知事件后，回送通知命令的正确

响应，事务标识（10002）与 MG 上报的通知命令（NTFY）的事务标识一致。证明 MGC 已正确收到 MG 上报的通知命令（NTFY）。

步骤 25：当 MGC 收到 MG 上报的加密结果，与自己计算的加密结果比较，如果 MG 上报的加密结果与 MGC 自己计算的加密结果一致。则认为该 MG 为合法的 MG，如果不一致或者 MG 在规定的时间内没有上报自己的加密结果，则认为该 MG 为非法的 MG。

权 利 要 求

1、一种网络安全认证方法，包括下述步骤：

步骤 1：媒体网关控制器（MGC）为媒体网关（MG）配置鉴权密钥，并且设置网络协议安全数据包；

步骤 2：在进行安全认证时，MGC 利用数据包(Package)向 MG 下发安全认证请求数据，MG 利用鉴权密钥对请求数据进行加密计算，并将计算结果反馈给 MGC；

步骤 3：MGC 根据认证结果确定被认证的 MG 是否合法。

2、根据权利要求 1 所述的网络安全认证方法，其特征在于：所述网络协议为媒体网关控制协议（MGCP）。

3、根据权利要求 1 所述的网络安全认证方法，其特征在于：所述网络协议为 H248 协议。

4、根据权利要求 1、2 或 3 所述的网络安全认证方法，其特征在于，所述数据包包括：安全认证请求信号和安全认证结果事件；所述安全认证请求信号中包括安全认证参数；安全认证结果 0 事件中包括安全结果认证参数。

5、根据权利要求 4 所述的网络安全认证方法，其特征在于，所述步骤 2 进一步包括：

步骤 21：MGC 下发数据包中的安全性认证请求信号给 MG；

步骤 22：MG 收到安全认证信号中的安全认证参数，使用鉴权密钥对上述参数进行加密计算，然后将加密计算结果通过数据包中的安全认证完成事件的安全结果认证参数上报给 MGC。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN03/00801

A. CLASSIFICATION OF SUBJECT MATTER

IPC [7]: H04L12/24 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC [7]: H04L12/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI EPODOC CNPAT PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2002087858 A (OLIVER N C, ET AL) 04 Jul 2002 (04.07.02) See all the document	1-5
A	JP2002247111 A (MCM JAPAN KK) 30 Aug 2002 (30.08.02) See all the document	1-5
A	US6353891 B (3COM CORP) 05 Mar 2002 (05.03.02) See all the document	1-5

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23.Dec 2003 (23.12.03)	25 DEC 2003 (25.12.03)
Name and mailing address of the ISA/CN 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-10-62019451	Authorized officer Wang Zhiwei Telephone No. 86-10-62084532

Form PCT/ISA /210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN03/00801

US2002087858 A	04.07.02	WO02054201 A	11.07.02
JP2002247111 A	30.08.02	None	
US6353891 B	05.03.02	None	

国际检索报告

国际申请号
PCT/CN03/00801

A. 主题的分类

IPC[7]：H04L12/24　H04L12/56

按照国际专利分类表(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类体系和分类号)

IPC[7]：H04L12/24

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称和，如果实际可行的，使用的检索词)

WPI　EPODOC　CNPAT　PAJ

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求编号
A	US2002087858 A （OLIVER N C 等） 04.7 月 2002（04.07.02） 说明书全文	1-5
A	JP2002247111 A （MCM JAPAN KK） 30.8 月 2002（30.08.02） 说明书全文	1-5
A	US6353891 B （3 柯姆公司） 05.3 月 2002（05.03.02） 说明书全文	1-5

☐ 其余文件在C栏的续页中列出。　☒ 见同族专利附件。

* 引用文件的专用类型：
"A" 明确叙述了被认为不是特别相关的一般现有技术的文件
"E" 在国际申请日的当天或之后公布的在先的申请或专利
"L" 可能引起对优先权要求的怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布的在后文件，它与申请不相抵触，但是引用它是为了理解构成发明基础的理论或原理
"X" 特别相关的文件，仅仅考虑该文件，权利要求所记载的发明就不能认为是新颖的或不能认为是有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，权利要求记载的发明不具有创造性
"&" 同族专利成员的文件

国际检索实际完成的日期	国际检索报告邮寄日期
23.12 月 2003（23.12.03）	25.12月 2003 (25.12.03)
国际检索单位名称和邮寄地址 ISA/CN 中国北京市海淀区西土城路 6 号(100088) 传真号：86-10-62019451	受权官员 王志伟 电话号码：86-10-62084532

国际检索报告
关于同族专利成员的情报

国际申请号
PCT/CN03/00801

检索报告中引用的专利文件	公布日期	同族专利成员	公布日期
US2002087858 A	04.07.02	WO02054201 A	11.07.02
JP2002247111 A	30.08.02	无	
US6353891 B	05.03.02	无	